EXHIBIT D

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

FEDERAL HOUSING FINANCE AGENCY, AS CONSERVATOR FOR THE FEDERAL NATIONAL MORTGAGE ASSOCIATION AND THE FEDERAL HOME LOAN MORTGAGE CORPORATION, Plaintiff, -v-. ALLY FINANCIAL INC. f/k/a GMAC LLC, *et al.*, Defendants.	11 Civ. 7010 (DLC)

Other Cases Brought By This Plaintiff:

11 Civ. 5201 (DLC)
11 Civ. 6188 (DLC)
11 Civ. 6189 (DLC)
11 Civ. 6190 (DLC)
11 Civ. 6192 (DLC)
11 Civ. 6193 (DLC)
11 Civ. 6195 (DLC)
11 Civ. 6196 (DLC)
11 Civ. 6198 (DLC)
11 Civ. 6200 (DLC)
11 Civ. 6201 (DLC)
11 Civ. 6202 (DLC)
11 Civ. 6203 (DLC)
11 Civ. 6739 (DLC)
11 Civ. 6916 (DLC)
11 Civ. 7048 (DLC)

This submission sets forth the proposal of Defendants Ally Financial Inc., GMAC Mortgage Group, Inc., Residential Capital LLC, GMAC-RFC Holding Company, LLC, Residential Funding Company, LLC, Ally Securities, LLC, Residential Asset Mortgage Products, Inc., Residential Asset Securities Corporation, and Residential Accredit Loans, Inc.

(the "Ally and ResCap Defendants") as to the treatment of discovery material containing mortgage loan borrowers' highly sensitive personally identifiable information ("PII") in the case brought by plaintiff FHFA against the Ally and ResCap Defendants currently pending before this Court. The Ally and ResCap Defendants' proposal supplements the proposed Protective Order materials submitted in the seventeen cases filed by FHFA that are pending before this Court (the "Cases"). Plaintiff has made clear in its submissions to this Court that it seeks to prioritize production of the origination and servicing files for the securitized loans at issue in the Cases. *See* Joint Report Regarding Certain Case Management Issues, No. 11 Civ. 5201 (Dkt. 71) at 5; Plaintiff FHFA's Proposal for Certain Case Management Issues, No. 11 Civ. 5201 (Dkt. 72) at 8-9. The Ally and ResCap Defendants' loan files, however, are replete with PII for the third-party individuals who took out the mortgages, including – but not limited to – borrower names, addresses, telephone numbers, Social Security numbers, credit card and bank account numbers, employment and salary data, monthly income, and descriptions of borrowers' debts and liabilities. This type of information is also captured in numerous spreadsheets, emails, and database information the Ally and ResCap Defendants anticipate producing in discovery. Ultimately, the Ally and ResCap Defendants expect that discovery in the Cases will involve the exchange of a substantial volume of PII.[1]

[1] Redaction of such information is not a practical solution, both due to the volume and diversity of material involved (not just whatever loan files are ultimately produced, but also spreadsheets – which are notoriously difficult to redact – and individual emails), and because in any event FHFA and the Ally and ResCap Defendants will need certain borrower-specific information to evaluate the loans. For example, if PII is redacted, there may be no practical way to match a given loan file up with email correspondence about a borrower or servicing records relating to that loan.

In the event of an unauthorized disclosure, scores of individual home mortgage borrowers – none of whom have *any* stake in this litigation – will be at significant risk of having their property or identity stolen and privacy invaded. Further, regardless of which party is responsible for the disclosure or whether there is even "fault" attributable to one party or another, the Ally and ResCap Defendants fear that they alone will be forced to bear the considerable remediation and reputational costs of such disclosures, as well as become the target of costly litigation by the borrowers whose PII was compromised. These risks are real, as demonstrated by the numerous real-life examples discussed below. These unique circumstances, and the extremely serious potential consequences for the Ally and ResCap Defendants and for third-party borrowers, render the standard bare promise to maintain certain disclosure protocols over sensitive discovery material insufficient. To address these risks and ensure that borrowers are adequately protected, the Ally and ResCap Defendants respectfully request that the Court enter the proposed Supplemental Protective Order governing PII that is attached to this submission as Exhibit A.

The proposed Supplemental Protective Order requires that all parties receiving PII from the Ally and ResCap Defendants agree either (a) to vetting by an independent security expert to ensure that adequate data protection controls are in place; or (b) to indemnify the Ally and ResCap Defendants in the event of an unauthorized disclosure of PII.[2] In two recent cases involving similar claims in which ResCap entities are parties and involving identical PII issues, the courts entered supplemental protective orders that applied such protections. In *New Jersey Carpenters Health Fund, et al. v. Residential Capital, LLC, et al.*, Case No. 08-CV-08781-HB

[2] In line with the proposed Protective Order submitted by the parties on April 27, 2012 (*see* Dkt. 86 and 87), which precludes the use of sensitive discovery material for any purpose other than the prosecution of the Actions, the proposed Supplemental Protective Order also prohibits the use of loan files or the data therein to contact borrowers or their accountants.

(S.D.N.Y.), after briefing, Magistrate Judge Ellis entered a protective order requiring plaintiffs to indemnify the defendants for any disclosure of PII. During a telephonic conference, Magistrate Judge Ellis observed that vetting and indemnification are two sides of the same coin, and that if plaintiffs were unwilling to agree to independent vetting (as was the case), it would be unfair to require defendants solely to bear the resulting risks. In *Nkengfack v. Homecomings Financial, LLC, et al.*, Case No. 03-C-09-007316 CN (Circuit Court for Baltimore County, MD), the court entered an order providing *greater* protections than Ally now seeks, requiring recipients of PII to submit to third-party vetting *and* to indemnify the party producing the PII. Other Courts have entered protective orders with similar provisions. *See, e.g., In re Honza,* 242 S.W.3d 578, 584 (Tex. Ct. App. 2008) (affirming confidentiality order and holding that requesting party's "expert must provide proof of being bonded and of having commercial liability insurance by which the Honzas may be fully indemnified against any monetary loss"); *Bradley v. Cooper Tire & Rubber Co.*, 2008 WL 5156616, at *4-5 (S.D. Miss. 2008) (entering a protective order that contained a fee-shifting provision in the event of unauthorized disclosure).

While their preference is for an order which requires both third-party vetting and indemnification, the Ally and ResCap Defendants seek a protocol which allows parties to choose between these measures.[3] The plaintiff, however, has refused to agree to this proposal, describing it as excessive and overly burdensome.[4]

---

[3] Co-defendants in both this and the related actions can, of course, also opt to forego receipt of larger volumes of PII-containing materials such as loan files and loan-level spreadsheets produced by Ally and ResCap, which are uniquely relevant to the claims and defenses involving the Ally and ResCap Defendants, thereby reducing their own risk.

[4] Certain defendants also do not agree, which is why the Ally and ResCap Defendants are submitting this proposal separately from the Defendants' main submission on protective order issues.

Plaintiff's position is not tenable. The production of non-trivial volumes of borrower PII in a large and complex multi-party case such as this raises unique challenges in managing and securing this data. For the Ally and ResCap Defendants, which are financial institutions charged with certain data protection obligations under federal and state law, the risk of another party's unauthorized disclosure of PII is real and significant. It is unreasonable and unfair to force the Ally and ResCap Defendants alone to face the extremely serious potential consequences of a data breach resulting from another party's possession and handling of the materials. Accordingly, the Ally and ResCap Defendants' proposed Supplemental Protective Order is necessary and warranted.

I. The Safeguards Provided In The Supplemental Protective Order Are Not Overly Burdensome.

The proposed security measures are no more (and in fact, quite a bit less stringent) than the security standards the Ally and ResCap Defendants use every day to safeguard this very same data. Indeed, as discussed below, *all* of the financial institution parties, as well as FHFA, apply similar security controls to their *own* data. Accordingly, requiring recipients of PII-containing data to apply the same protections to those materials produced by the Ally and ResCap Defendants is not especially burdensome.

Under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* ("GLBA"), financial institutions have "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. The statutory definition of "financial institution" brings within its scope all entities that engage in activities that are "financial in nature," including but not limited to loans, financial or investment advice, insurance, and sales, trading, or underwriting of securities and other financial products. 15 U.S.C. § 6809(3)(A) (incorporating the list of

financial activities set out in 12 U.S.C. § 1843(k)). This definition clearly encompasses the Ally and ResCap Defendants. The FTC's implementing regulations for § 6801 mandate that each financial institution "develop, implement, and maintain a comprehensive information security program" that "[i]nsure[s] the security and confidentiality" of PII and protects against "anticipated threats or hazards to the security or integrity of such information" or "unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer." 16 C.F.R. § 314.3.[5] In addition to the GLBA, financial institutions are subject to a web of state laws and regulations that impose sector-specific and data-specific requirements on the use and disclosure of PII. *See, e.g.,* Cal. Civ. Code §§ 1798.80-1798.84, 1798.85-1798.86; Conn. Gen. Stat. § 36a-701b & P.L. No. 08-167; Fla. Stat. § 817.5681; Ill. Comp. Stat. §§ 530/1-40; Mass. Gen. Law ch. 93H & Mass. 201 CMR 17.00; Mich. Comp. Laws §§ 445.72, 445.84, 445.86; N.J. Stat. §§ 56:8-161, 163-166; N.Y. Gen. Bus. Law § 899-aa; Va. Code Ann. § 18.2-186.6; Wash. Rev. Code §§ 19.255.010-020.[6]

---

[5] The Gramm-Leach-Bliley Act contains a "judicial process" exception. However, that exception appears to apply only to the requirement that financial institutions give customers notice and an opportunity to opt out before the institution may release PII. 15 U.S.C. §§ 6802(b), (e)(8); 16 C.F.R. § 313.15(a)(7)(iii). In other words, the Ally and ResCap Defendants need not pre-notify borrowers that their personal information is about to be shared with other parties in the litigation. However, it is by no means clear that the judicial exception has any effect whatsoever on the Ally or ResCap Defendants' safeguarding duties, or that it precludes the potential penalties and consumer lawsuits that may result from an unauthorized disclosure.

[6] Although certain of the states simply set out certain notification requirements in the event of a data breach (which themselves can be costly to implement), other states impose affirmative security requirements. California's law requires every "business that owns or licenses personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and "protect the personal information from unauthorized access, destruction, use, modification or disclosure." Cal. Civ. Code § 1798.81.5(b). Such businesses also are responsible for ensuring that third parties receiving PII follow these same requirements. *Id.* § 1798.81.5(c). The Commonwealth of Massachusetts requires businesses that store or use personal information about that state's

The Ally and ResCap Defendants comply with these requirements in the daily course of business through the use of industry-standard security policies and protocols.[7]

Similarly, FHFA is required by the Federal Information Security Management Act of 2002 ("FISMA"), 44 U.S.C. § 3541 *et seq.*, to apply a stringent set of mandatory security controls applicable to the information systems of all federal agencies (except those related to national security). *See* 44 U.S.C. § 3543(a) (requiring the Director of the Office of Management and Budget to promulgate security controls for all systems other than those related to national security); *see also* National Institute of Standards and Technology's (NIST) Special Publication 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and*

---

residents to develop and use a "comprehensive information security program." Mass. 201 CMR 17.03(1). The regulation allows a business to tailor its program to its size and resources, but certain components – including procedures requiring "third-party service providers by contract to implement and maintain such appropriate security measures for personal information" – must be included. *Id.* 17.03(2)(f)(2).

[7] Ally Financial, Inc. also is a member of BITS, an organization created by a number of the world's largest financial institutions to act as the technology policy division of The Financial Services Roundtable. One of the key initiatives of BITS is to create and release information security guidelines for the financial industry, and according to testimony by BITS President Leigh Williams at a June 2011 Senate hearing on "Cybersecurity and Data Protection in the Financial Sector," BITS members voluntarily have undertaken to implement strict protocols for the protection of customer data. Mr. Williams emphasized that this effort "is not seen by industry executives as discretionary or optional. The market, good business practices and prudence all require it." Williams, Leigh. Statement to the Senate, Committee on Banking, Housing, and Urban Affairs. *Cybersecurity and Data Protection in the Financial Sector*, Hearing, June 21, 2011. Available at http://banking.senate.gov/public/_index.cfm?FuseAction=Files.View&FileStore_id=683be265-4cd4-4f93-a563-77709a52836c (accessed 3/26/12). Many of the largest defendants in the Cases (or those defendants' parents) are members of BITS, including Bank of America Corp., Barclays Capital, Inc., Citigroup Inc., General Electric Co., HSBC North America Holdings, Inc., JPMorgan Chase & Co., The PNC Financial Services Group, Inc., RBS Americas, and Wells Fargo & Company. Accordingly, for many (if not all) of the other defendants, it is doubtful that the third-party verification option in the Proposed Supplemental Protective Order would require dramatic changes in those parties' data protection programs. It is not unreasonable to expect parties' outside consultants and experts to adhere to the same degree of caution.

Organizations (providing comprehensive recommendations for security controls to implement FISMA).[8] Thus, FHFA cannot reasonably claim that it is beyond its capability to implement the security standards appropriate for PII.

II. The Threat Of A Data Breach Is Real And Poses Serious Risks For The Third-Party Borrowers.

The Ally and ResCap Defendants' loan files contain precisely the type of information that facilitates identity theft, a problem that affects approximately 9 million U.S. residents every year. *See* FTC "About Identity Theft" website, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html; *see also* Department of Justice Bureau of Justice Statistics "Identity Theft Reported by Households, 2005-2010" (Nov. 2011), *available at* http://www.bjs.gov/content/pub/pdf/itrh0510.pdf (8.7 million U.S. households, or approximately 7.0% of the population, reported at least one instance of identity theft in 2010). As the National Institute of Standards and Technology (which develops the security controls for FHFA and other federal agencies controlled by FISMA) notes:

> The escalation of security breaches involving [PII] has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs.

National Institute of Standards and Technology "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," Special Publication 800-122, at ES-1.

---

[8] FISMA also requires yearly independent audits of the information security programs and practices of all federal agencies, including FHFA. 44 U.S.C. § 3535. As described in more detail below and in the audit report attached as Exhibit B, a September 2011 audit found that FHFA's security controls were "not fully effective to preserve the confidentiality, integrity and availability of FHFA's information and information systems." *See* Exhibit B at 4.

Unfortunately, the threat of an inadvertent disclosure of PII in this litigation is neither imaginary nor remote. According to the Privacy Rights Clearinghouse Chronology of Data Breaches,[9] in the past five years (between January 2007 and December 2011), the financial and insurance services industry made public 206 breaches due to unintended disclosure, hacking/malware, loss/theft of documents or a data repository, or unknown causes, implicating 166,243,754 records. For example:

- In July 2011, CD-ROMs containing the PII of 34,000 Morgan Stanley customers were lost.
- In June 2011 hackers obtained the PII of 360,000 Citibank customers.
- In June 2009, a computer containing the PII of several current and former Merrill Lynch financial advisors was stolen from the home of a third-party consultant.
- In September 2007, a Citigroup employee inadvertently leaked Social Security numbers and other personal data for 5,200 customers over an online file-sharing network.
- In May 2007, a computer tape containing PII for 47,000 JP Morgan clients and employees was lost in transfer to off-site storage.
- In February 2007, Credit Suisse inadvertently posted PII for 3,000 loan applicants online, including Social Security numbers and credit scores.

During the same period, federal and state government entities made public 341 breaches due to the same grounds, implicating 96,692,081 records. For example:

- In April and October 2011, media reports revealed that the Social Security Administration accidentally had included the full names, Social Security numbers, birth dates, and last known zip codes for nearly 100,000 living U.S. citizens in the SSA's "Death Master File."

---

[9] The Privacy Rights Clearinghouse, a nonprofit consumer organization, compiles a publicly-available Data Breach Chronology primarily from a list-serve maintained by the Open Security Foundation, which includes data from verifiable media reports, government websites, FOIA requests, and blog posts. *See* Chronology of Data Breaches FAQ, *available at* https://www.privacyrights.org/data-breach-FAQ. All of the breaches described in this submission are listed on the Chronology.

- In June 2010, the National Highway Traffic Safety Administration made the PII for an unknown number of citizens, including Social Security numbers, addresses and drivers' license numbers, available in a public complaint database.
- In May 2010, a laptop containing the unencrypted PII for 616 veterans was stolen from the home of a Department of Veterans Affairs contractor.
- In December 2009, a laptop containing PII for 42,000 individuals was stolen from a U.S. Army employee.
- In October 2009, the U.S. Military Veterans agency disclosed the PII of 76 million veterans, including millions of Social Security numbers, on a hard drive returned to a vendor.
- In August 2009, a National Finance Center employee compromised the PII of 27,000 Commerce employees through transmission in unencrypted form.
- In May 2009, the National Archives and Records Administration lost a hard drive containing PII for 250,000 federal employees.
- In February 2009, hackers accessed 48,000 names and Social Security numbers from a Federal Aviation Administration database.
- In December 2008, the Federal Emergency Management Agency experienced a breach resulting in release of PII for nearly 17,000 individuals, and the U.S. Army lost a laptop containing PII for as many as 6,000 individuals.
- In June 2008, a laptop and hard drive containing PII for 800-900 soldiers was stolen from a U.S. Army employee's truck.
- In December 2007, a laptop containing PII for 10,500 members and veterans was stolen from the home of a U.S. Air Force employee.
- In May 2007, the Transportation Security Administration lost a hard drive containing payroll data for 100,000 current and former employees, including Social Security numbers, dates of birth, and bank account and routing information.

FHFA itself faces a serious risk of a breach in its data systems. An independent audit of FHFA dated September 29, 2011 found that "information security practices were not fully effective to preserve the confidentiality, integrity and availability of FHFA's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Exhibit B at 4. Specifically, the audit found that FHFA had failed to (1) finalize, disseminate, and implement an organization-wide security program

plan; (2) update its information systems policies and procedures to comply with the most current federally-mandated standards; (3) develop a methodology for categorizing data by type; (4) implement adequate procedures for tracking and monitoring security weaknesses, or (5) implement adequate procedures for tracking and monitoring the remediation of security weaknesses. *Id.* The audit concluded that these deficiencies are "significant" and increase the risks of inconsistent data handling and unauthorized data access, manipulation, or deletion. *Id.* at 19, 22, 24, 26-27, 33. Most troubling, the report found "a high number of vulnerabilities" in the agency's support systems, and that "FHFA management did not place a priority on monitoring the remediation process to ensure th[at] weaknesses … were tracked … and remediated." *Id.* at 29-30. The audit warned that "[t]he vulnerabilities that were not remediated could lead to total system compromise." *Id.* at 30.

Nor are lawyers and experts immune from data breach risks. For example:

- In October 2011, an employee of a Baltimore law firm lost a hard drive containing PII and medical information for an unknown number of individuals.
- In May 2011, a laptop in the custody of an expert witness in litigation between two dental services providers was stolen, disclosing the PII of thousands of patients.
- In June 2006, a laptop containing Social Security numbers and other PII for an unknown number of individuals was stolen from a lawyer for the Social Security Administration, who had violated agency protocol by bringing the laptop to a conference.

Given this history, none of the parties in this litigation credibly can claim that an inadvertent disclosure of PII is impossible, or that the risk of such a disclosure is negligible. To the contrary, the indisputable conclusion is that such breaches occur regularly, and that the measures outlined in the Proposed Supplemental Protective Order are necessary and prudent.

III. A Data Breach Could Have Extremely Serious Adverse Consequences For The Ally and ResCap Defendants.

The Ally and ResCap Defendants potentially face substantial economic and reputational damages, as well as costly private litigation, if any party in the Cases loses, misplaces, exposes, or otherwise discloses PII produced by the Ally and ResCap Defendants. Whether a data breach is due to criminal activity, negligence, or accident is irrelevant: regardless of the circumstances, the relevant authorities and the individuals whose PII was disclosed will initially turn to the Ally and ResCap Defendants for remediation and recourse.

46 states and the District of Columbia have enacted breach notification statutes that generally require any entity that collected PII from a customer to provide notification of any breach compromising that data, with significant civil and even criminal penalties for noncompliance. *See, e.g.,* Cal. Civ. Code § 1798.82; Conn. Gen. Stat. § 36a-701b; Fla. Stat. § 817.5681; Ill. Comp. Stat. §§ 530/10; Mass. ch. 93H § 3; Mich. Comp. Laws §§ 445.72; N.J. Stat. §§ 56:8-163; N.Y. Gen. Bus. Law § 899-aa; Va. Code Ann. § 18.2-186.6; Wash. Rev. Code §§ 19.255.010-010. Complying with these measures is expensive; current data puts the average cost of remediation in the event of an unauthorized disclosure by any party in this case at $73 *per name*. *See* Ponemon Institute, Sixth Annual US Cost of Data Breach Study (2011) (attached as Exhibit C). Even assuming that each loan file involved only a single borrower, which is unlikely, if, say, FHFA's expert loses a hard drive containing spreadsheets or other loan-level data for just the loans directly at issue for the Ally and ResCap Defendants, the cost *to the Ally and ResCap Defendants* could exceed *$8 million*, *plus* any applicable federal or state monetary penalties.

This $73 per name figure does not include the potentially substantial damage the Ally and ResCap Defendants' reputations may sustain even if they bear no fault for the breach. In a recent global survey, one in five U.S. respondents stated that they would stop doing business with a

bank, credit card company, or retailer that sustained a security breach, regardless of the circumstances. *See* SailPoint, "2011 SailPoint Market Pulse Survey – The Data Breach Battle," *available at* http://www.sailpoint.com/2011survey/ (accessed 3/26/12). Further, 10% of U.S. respondents not only would refuse to do further business with that organization, but also would advise their family and friends to do the same.

Another party's unauthorized disclosure also subjects the Ally and ResCap Defendants to the risk of consumer litigation. Certain of the applicable state statutes authorize such suits, as well as suits by the state attorneys general. *See, e.g.,* Cal. Civ. Code § 1789.84 (authorizing private civil actions, with enhanced monetary per-violation penalties for willful and intentional conduct).[10]

Regardless of the Ally and ResCap Defendants' actual potential for statutory liability for another party's unauthorized disclosure, it is clear that individuals have not hesitated to bring lawsuits in the wake of unauthorized disclosure of PII. Several such cases currently are proceeding in the federal courts. *See, e.g., Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (class action brought following the hacking of 4.2 million credit and debit card numbers, expiration dates, and security codes from a grocery chain database); *In re Michaels Stores Pin Pad Litig.*, No. 11 C 3350, 2011 WL 5878373 (N.D. Ill. Nov. 23, 2011) (class action

---

[10] No court has considered whether or how a financial institution would be liable under the GLBA for the inadvertent disclosure of PII following production pursuant to a protective order. However, there is a rational basis on which a court could reach that conclusion. The FTC "Safeguards Rule," codified at 16 C.F.R. §§ 314.1-314.5, imposes upon financial institutions a continuing legal obligation to protect the PII in their custody against anticipated security threats and unauthorized access. 16 C.F.R. § 314.3. Of particular interest is the FTC's rule obligating custodians to exercise oversight in selecting and imposing contractual safeguards on third-party PII recipients (described in the rule as "service providers"). 16 C.F.R. § 314.4(d). While the Ally and ResCap Defendants may well have valid counter-arguments to such liability, nonetheless, the costs and risks entailed in defending against such litigation are significant.

brought by consumers whose debt and credit card data was stolen through PIN pad tampering); *In re Heartland Payment Sys., Inc. Cust. Data Sec. Breach Litig.*, MDL No. 09-2046 (S.D. Tex. Mar. 20, 2012)) (approving class action settlement of litigation brought by credit card banks and cardholders following the hacking of credit card information for more than 1 million consumers from a credit card transaction processor's database; defendants agreed to pay up to $2.4 million in damages and over $600,000 in legal fees to class counsel). Whether or not such individual lawsuits raise valid claims, and regardless of the strength of the Ally and ResCap Defendants' potential defenses to such suits, such litigation – particularly when brought in the form of a class action – can be enormously expensive to defend. As the Court is well aware, even a facially noncognizable claim can take many months and tens or even hundreds of thousands of dollars in fees and costs to dismiss. Under the standard protective order proposed by FHFA and the other Defendants, these costs unfairly would be borne by the Ally and ResCap Defendants alone even if the data at issue was stolen from or inadvertently disclosed by FHFA, its experts or consultants, or some other party.

IV. The Ally and ResCap Defendants Have No Certain Legal Remedy For Another Party's Unauthorized Disclosure Of Its Borrowers' PII.

For all these reasons, a court order permitting or requiring the Ally and ResCap Defendants to disclose PII to other parties, not to mention those parties' experts, consultants, and other third-party associates, affords little protection to the Ally and ResCap Defendants. The existence of such an order does not immediately obviate any remediation obligations that may apply, and cannot prevent lawsuits from being filed. None of the other parties has identified, and the Ally and ResCap Defendants have not discerned, a fail-safe basis through which the Ally and ResCap Defendants could displace liability following an unauthorized disclosure onto the disclosing party. The potential availability of sanctions under the Federal Rules is unlikely to be

able to address a scenario in which disclosure is the result of negligence or the wrongdoing of a non-party, rather than the custodial party's own deliberate wrongdoing or recklessness. Thus, absent the protections set forth in the Supplemental Protective Order, there is no guarantee that others could be made to bear either the risks or the costs of their own or their agents' unauthorized disclosures. Nor is it reasonable, where FHFA is the party seeking access to such voluminous amount of private consumer information, to place the burden on the Ally and ResCap Defendants to find some remedial scheme to address data breaches that may occur while that information is in the possession or control of FHFA.

Finally and equally important, the proposed Supplemental Protective Order provides the greatest available protection to consumers. Simply put, a party that has agreed *ex ante* to maintain tight security protocols over PII or to indemnify the Ally and ResCap Defendants in the event of a disclosure faces a concrete risk, and doubtless will devote considerably more attention to safeguarding that data than a party facing the vague possibility of some sort of *post-hoc* shifting of liability under an undefined theory.

In sum, past experience demonstrates that there is a significant risk that PII produced by the Ally and ResCap Defendants in this case could be breached or otherwise disclosed by one of the receiving parties, and that this could result in disclosure of personal information for thousands of consumers. The financial and reputational risk of such a disclosure to consumers, to the Ally and ResCap Defendants, and indeed to all involved in this litigation, requires a heightened vigilance to ensure that adequate safeguards against the disclosure of PII are in place. The law and the equities, as well as the actual circumstances of the parties, favor entry of a supplemental protective order tailored to address the risks posed by unauthorized disclosure of

borrowers' PII. The Ally and ResCap Defendants respectfully request that the Court enter the proposed Supplemental Protective Order attached hereto as Exhibit A.

Dated: May 1, 2012
New York, NY

Respectfully submitted,

_/s/ David Potter_____
David Potter (dpotter@lpgllp.com)
LAZARE POTTER & GIACOVAS LLP
950 Third Avenue
New York, NY 10022

and

Jeffrey A. Lipps (lipps@carpenterlipps.com)
Jennifer A.L. Battle (battle@carpenterlipps.com)
CARPENTER, LIPPS & LELAND LLP
280 Plaza, Suite 1300
280 North High Street
Columbus, OH 43215

Attorneys for Residential Capital LLC, GMAC-RFC Holding Company, LLC, Residential Funding Company, LLC, Ally Securities, LLC, Residential Asset Mortgage Products, Inc., Residential Asset Securities Corporation, and Residential Accredit Loans, Inc.

_/s/ Richard A. Spehr_____
Richard A. Spehr (rspehr@mayerbrown.com)
Michael O. Ware (mware@mayerbrown.com)
MAYER BROWN LLP
1675 Broadway
New York, NY 10019

Attorneys for Ally Financial Inc. and GMAC Mortgage Group, Inc.